AMENDMENTS TO THE SPECIFICATION

Please replace paragraph [0012] with the following amended paragraph:

To perform cryptographic operations on multiple successive blocks of text, all of the symmetric key algorithms employ the same types of modes. These modes include electronic code book (ECB) mode, cipher block chaining (CBC) mode, cipher feedback (CFB) mode, and output feedback (OFB) mode. Some of these modes utilize an additional initialization vector during performance of the sub-operations and some use the ciphertext output of a first set of cryptographic rounds performed on a first block of plaintext as an additional input to a second set of cryptographic rounds performed on a second block of plaintext. It is beyond the scope of the present application to provide an in depth discussion of each of the cryptographic algorithms and sub-operations employed by present day symmetric key cryptographic algorithms. For specific implementation standards, the reader is directed to Federal Information Processing Standards Publication 46-3 (FIPS-46-3), dated October 25, 1999 for a detailed discussion of DES and Triple DES, and Federal Information Processing Standards Publication 197 (FIPS-197), dated November 26, 2001 for a detailed discussion of AES. Both of the aforementioned standards are issued and maintained by the National Institute of Standards and Technology (NIST) and are herein incorporated by reference for all intents and purposes. In addition to the aforementioned standards, tutorials, white papers, toolkits, and resource articles can be obtained from NIST's Computer Security Resource Center (CSRC) over the Internet ~~at http://csrc.nist.gov/~~.

Please delete the section entitled "SUMMARY OF THE INVENTION" in its entirety and substitute the following section therefor:

SUMMARY OF THE INVENTION

[0020.1] The present invention, among other applications, is directed to solving these and other problems and disadvantages of the prior art. The present invention provides a superior technique for performing cryptographic operations within a microprocessor. In one embodiment, an apparatus for performing cryptographic operations is provided. The apparatus includes an x86-compatible microprocessor. The x86-compatible

microprocessor has an instruction register having a cryptographic instruction disposed therein, a keygen unit, and an execution unit . The instruction register is within the ~~microprocessor~~x86-compatible microprocessor and has a cryptographic instruction disposed therein. The cryptographic instruction is part of an application program, and the ~~microprocessor~~x86-compatible microprocessor executes the application program. The cryptographic instruction prescribes one of the cryptographic operations, is arranged according to the instruction format for execution on the x86-compatible microprocessor, and also prescribes that a user-generated key schedule be employed when executing the one of the cryptographic operations. The keygen unit is operatively coupled to the instruction register. The keygen unit directs the ~~microprocessor~~x86-compatible microprocessor to load the user-generated key schedule. The execution unit is operatively coupled to the keygen unit. The execution unit employs the user-generated key schedule to execute the one of the cryptographic operations. The execution unit includes a cryptography unit that is configured execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, where the plurality of cryptographic rounds are prescribed by a control word that is provided to the cryptography unit.

[0021] One aspect of the present invention contemplates an apparatus for performing cryptographic operations. The apparatus has a cryptography unit within a ~~microprocessor~~x86-compatible microprocessor and a keygen unit. The cryptography unit executes one of the cryptographic operations responsive to receipt of a cryptographic instruction within an application program that prescribes the one of the cryptographic operations, ~~wherein~~ where the cryptographic instruction is arranged according to the instruction format for execution on the x86-compatible microprocessor, and where the ~~microprocessor~~x86-compatible microprocessor executes the application program. The cryptographic instruction also prescribes that a user-generated key schedule be employed when executing the one of the cryptographic operations. The keygen unit is operatively coupled to the cryptography unit. The keygen unit directs the ~~microprocessor~~x86-compatible microprocessor to perform the one of the cryptographic operations and to

employ the user-generated key schedule when performing the one of the cryptographic operations.

[0022] Another aspect of the present invention provides a method for performing cryptographic operations in a ~~microprocessor~~x86-compatible microprocessor. The method includes executing an application program that is stored in memory, where the executing includes receiving a cryptographic instruction from the memory that prescribes employment of a user-generated key schedule during execution of one of a plurality of cryptographic operations and within a cryptographic unit in the ~~microprocessor~~x86-compatible microprocessor. The cryptographic instruction is arranged according to the instruction format for execution on the x86-compatible microprocessor. The method also includes employing the user-generated key schedule when executing the one of the cryptographic operations to generate a result of the one of the cryptographic operations.